EL TEOREMA DE FERMAT

Capi Corrales Rodrigáñez

En el año 1993, y casi por primera vez en la historia, una noticia sobre matemáticas invadió los medios de comunicación: el teorema de Fermat, que durante casi cuatrocientos años había resistido los esfuerzos de legos y profanos, estaba prácticamente demostrado. Andrew Wiles había presentado en Cambridge, Inglaterra, la *maqueta* de una demostración ante expertos de todo el mundo, y éstos habían concluido que la construcción -culminada de hecho con éxito por el propio Wiles año y medio más tarde- era factible.

En el siglo XVII la teoría de los números no se estudiaba en Universidades. Casi todos los matemáticos dedicados a los números en Europa (en aquel momento eran todos varones, aunque no siempre fue así antes, ni ha sido así después) tenían profesiones paralelas, Fermat era letrado, y habían establecido una red epistolar alrededor del jesuita Mersenne. Algo parecido a las redes de correo electrónico de hoy en día. A través de esta red se retaban con problemas los unos a los otros. ([G-1]). Pierre de Fermat fue uno de los individuos más activos en este grupo. A su muerte, su hijo publicó sus apuntes, entre ellos el enunciado de su famoso teorema, escrito a pluma en el margen de un ejemplar de *Aritmética* de Diofanto (S. II d. C.): "No es posible encontrar dos cubos cuya suma sea un cubo, dos potencias cuartas cuya suma sea una potencia cuarta y, en general, dos potencias cuya suma sea una potencia del mismo tipo. He descubierto una demostración verdaderamente maravillosa de este hecho, que no cabe en este margen" ([F]).

Hay infinitas ternas (x,y,z) de números enteros tales que $x^2 + y^2 = z^2$, como (3,4,5) o (12,5,13). Fermat asegura que no es posible hallar x,y,z enteros y no nulos tales que $x^3 + y^3 = z^3$, ó $x^4 + y^4 = z^4$, ó $x^5 + y^5 = z^5$, etc.

Desde que se publicara la nota de Fermat, muchos han intentado sin éxito encontrar la demostración que en su nota Fermat afirma haber hallado. La opinión de los especialistas es que, o bien Fermat se estaba marcando un farol, o bien había dado con una solución equivocada ([AC] pp. 1-22). Quizás la que, a finales del siglo pasado, propuso el alemán Kummer. Kummer demostró la afirmación de Fermat para $n < 100$ ([R], [AC] pp. 33-43) y, como tantos otros, creyó en un momento dado haber demostrado el teorema (es decir, para todo valor de n). Al repasar sus argumentos, además de un error, Kummer encontró otra cosa: un nuevo tipo de objetos matemáticos, a los que llamó números ideales. Los ideales de Kummer supusieron el nacer de la teoría de los números algebraicos y de la geometría algebraica, marco matemático en el que el teorema de Fermat ha sido demostrado. El camino seguido para llegar a la demostración tiene tres tramos fundamentales:

1. *Entre los años 50 y 60, Taniyama, Shimura y Weil perfilan una conjetura: todas las curvas de un cierto tipo que llamaremos E* (las curvas elípticas, de

ecuación $y^2 = x^3 + Ax^2 + Bx + C$ con coeficientes racionales y discriminante no nulo), *tienen una cierta propiedad que llamaremos P* (son modulares).

Las funciones trigonométricas $x(t) = sen\, t$, $y(t) = cos\, t$, parametrizan los puntos del círculo $x^2 + y^2 = 1$: al ir tomando t distintos valores reales, el par $(x(t), y(t))$ va recorriendo los puntos del círculo. La conjetura de Taniyama-Shimura-Weil predice que dada una curva elíptica E: $y^2 = x^3 + Ax^2 + Bx + C$, existen dos funciones modulares $x(z)$, $y(z)$ —funciones definidas en el plano superior complejo con propiedades especiales de periodicidad— que la parametrizan: al ir tomando z distintos valores complejos con su parte imaginaria $Im(z) > 0$, el par $(x(z),y(z))$ va recorriendo los puntos de la curva E ([G-2], [AC] pp. 59-79). Expresamos esta propiedad diciendo que la curva E es modular.

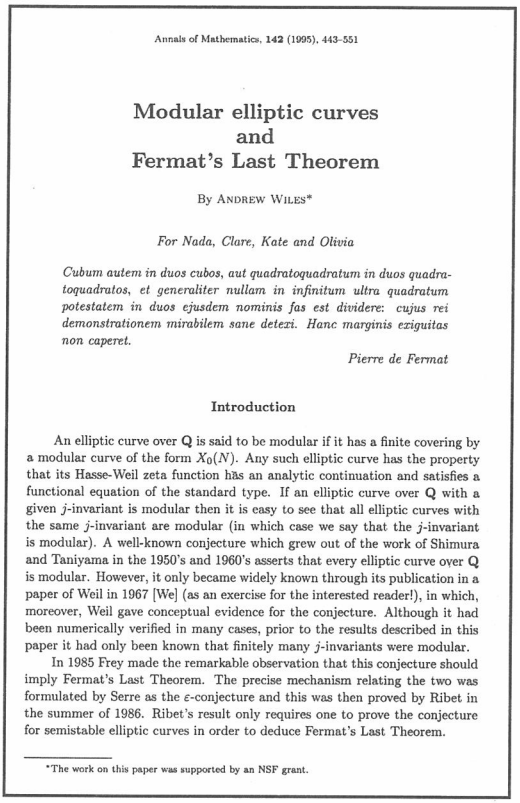
2. *A mediados de los ochenta, Frey predijo y Ribet demostró que cualquier solución entera a la ecuación de Fermat para n> 5 daría lugar a una curva de tipo E sin la propiedad P.* Más específicamente, G. Frey sugirió que si pudiésemos encontrar tres números *a, b, c* tales que $a^n + b^n = c^n$ con $n > 5$, la curva elíptica $y^2 = x(x - a^n)(x + b^n)$ no sería modular. En 1986 K. Ribet demostró esta afirmación, abriendo con ello una nueva vía para demostrar el teorema de Fermat: demostrar la conjetura de Taniyama-Shimura-Weil.

3. *En octubre de 1994, A. Wiles demostró,* utilizando prácticamente todos los resultados obtenidos en la década previa en geometría algebraica aritmética y teoría de los números algebraicos-, *la conjetura de Taniyama-Shimura-Weil para algunas de las curvas de tipo E. En particular, para la que surgiría a partir de una hipotética solución a la ecuación de Fermat.* Por lo tanto, tal solución no puede existir, pues de existir *daría lugar a una curva E a la vez con la propiedad P y sin la propiedad P.* Absurdo ([Wi], [AC] pp. 117-136).

95

Hay muchas personas a las que ha entristecido que este teorema haya sido resuelto. Para ellas, se ha roto un sueño. Y para colmo, la demostración no es intuitiva, no deslumbra, no se puede comercializar y, encima, parece que la entienden sólo una mínima parte de los matemáticos. ¿No habremos matado a cañonazos a un ejemplar bello y valiente? Quizás. Pero en estos tiempos que corren, somos muchas las personas dentro del mundo de la matemática a quienes llena de esperanza el que la modernísima -por lo muy modernas y recientes que son las herramientas que utiliza- demostración del teorema de Fermat, haya tenido lugar *a la antigua*, fuera de las modas y corrientes imperantes hoy en el mundo de la investigación. Porque si el teorema de Fermat es un clásico, clásica es también, a pesar de su modernidad, su demostración. Por tres razones.

1. En un momento en el que lo que más se fomenta es el hacer competitivo, la lucha sin cuartel por la fama y la gloria del individuo aislado con nombre y apellidos, el teorema de Fermat, el más famoso teorema de la matemática, *se ha resuelto gracias al trabajo de muchos.* La demostración final ha resultado ser un bellísimo encaje de bolillos en el que Wiles combina resultados y piezas conseguidas por las más brillantes y astutas cabezas del pensar matemático contemporáneo, además de sus propios resultados. La demostración de Wiles no cabe en el margen de una página, entre otras cosas, porque la lista



Annals of Mathematics, **142** (1995), 443-551

Modular elliptic curves and Fermat's Last Theorem

By Andrew Wiles*

For Nada, Clare, Kate and Olivia

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere: cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Pierre de Fermat

Introduction

An elliptic curve over **Q** is said to be modular if it has a finite covering by a modular curve of the form $X_0(N)$. Any such elliptic curve has the property that its Hasse-Weil zeta function has an analytic continuation and satisfies a functional equation of the standard type. If an elliptic curve over **Q** with a given j-invariant is modular then it is easy to see that all elliptic curves with the same j-invariant are modular (in which case we say that the j-invariant is modular). A well-known conjecture which grew out of the work of Shimura and Taniyama in the 1950's and 1960's asserts that every elliptic curve over **Q** is modular. However, it only became widely known through its publication in a paper of Weil in 1967 [We] (as an exercise for the interested reader!), in which, moreover, Weil gave conceptual evidence for the conjecture. Although it had been numerically verified in many cases, prior to the results described in this paper it had only been known that finitely many j-invariants were modular.

In 1985 Frey made the remarkable observation that this conjecture should imply Fermat's Last Theorem. The precise mechanism relating the two was formulated by Serre as the ε-conjecture and this was then proved by Ribet in the summer of 1986. Ribet's result only requires one to prove the conjecture for semistable elliptic curves in order to deduce Fermat's Last Theorem.

*The work on this paper was supported by an NSF grant.

Portada del artículo de Andrew Wiles con la solución del teorema de Fermat aparecido en la revista Annals of Mathematics *en 1995.*

de personas que han hecho posible con sus trabajos tal demostración necesita por sí misma todo un libro (Barry Mazur en [S]).

2. Cada vez es más frecuente que los problemas matemáticos tengan enunciados tan difíciles y especializados que, tan sólo para entender qué nos están diciendo, se necesiten años de estudios. Si en muchos casos esta situación es inevitable, en otros tantos es fruto de la moda del momento. El teorema de Fermat es un teorema de *enunciado sencillo y asequible.* Y sin embargo, para ser resuelto ha necesitado de algunas de las técnicas más sofisticadas de la matemática del siglo XX.

3. En matemáticas es cada vez más difícil el dedicarse al estudio de problemas que requieran *muchos años de estudio y labor.* La presión a publicar por publicar, ya sea dejando resultados a medias, ya sea cortando otros en diez trozos que den lugar a otros tantos artículos es cada vez más fuerte. Más de trescientos años se ha tardado en resolver el teorema de Fermat. Y se ha resuelto gracias a las miles de horas que miles de individuos han dedicado a su estudio sin conseguir nada publicable a cambio.

El teorema está demostrado. Un teorema que a lo largo de los últimos siglos ha dado lugar a gran cantidad de matemática, bellísima y profunda ([R]). Además, siguiendo la estrategia de Wiles, los matemáticos Breuil,

Conrad, Diamond y Taylor demostraron en 1999 la conjetura de TSW para todas las curvas elípticas. Si el teorema de Fermat no tiene ninguna aplicación práctica, no ocurre lo mismo con la conjetura de Taniyama-Shimura-Weil. Su demostración supone un paso importantísimo en el Programa Langlans, un proyecto de efecto fundamental para la matemática, surgido en este siglo, y que consiste en asociar a una estructura algebraica (en este caso una curva elíptica) un tipo específico de serie infinita construida a partir de datos concretos de la estructura (la serie L de la curva, que la conjetura de Taniyama-Shimura-Weil relaciona específicamente con su parametrización modular), y estudiar la información que la una brinda sobre la otra.

Pero no sólo la matemática se ha beneficiado con el teorema de Fermat. Pensemos en los miles de individuos que a lo largo de los años le han dedicado su tiempo. Durante las horas que le dedicaban al teorema, estas personas han vivido en la frontera de su ser, en el límite de las capacidades de su razón. Se han atrevido a dejar atrás el terreno de las certidumbres para saltar en el espacio de las aventuras abstractas. No es fácil. ¿Quién no se ha sentido paralizado de miedo ante un papel y un lápiz, aún estando a solas en una habitación? Al penetrar en terreno nunca antes pisado por ser humano, ya sea en la jungla como en la matemática, se dejan atrás las referencias, las coordenadas. Se vuela con la libertad del pájaro a quien no preocupa que el cielo sea ilimitado. En el hacinamiento físico, mental y espiritual de esta sociedad nuestra, el viaje matemático no es una pérdida de tiempo. Es ala con la que volar, y es raíz con la que afianzarse.

Tus pies sobre la tierra antes no hollada,
Tus ojos frente a lo antes nunca visto.

Peregrino, Luis Cernuda.

95

Mi experiencia al hacer matemáticas es la de entrar en una mansión a oscuras. Entras en la primera habitación y está a oscuras, completamente a oscuras. Tropiezas con los muebles, te tambaleas. Poco a poco aprendes donde está cada mueble. Y finalmente, tras unos seis meses, encuentras el interruptor y das la luz. De repente todo se ilumina y puedes ver donde estás exactamente. Entonces entras en la siguiente habitación a oscuras...

Andrew Wiles ([S])

Bibliografía

[AC] Andradas, C.; y Corrales Rodrigáñez, C. (Eds.): *400 años de matemáticas en torno al Teorema de Fermat.* Ed. Complutense, Madrid 1999.

[F] Fermat, P. de: *Œuvres.* Tannery y Henry eds., pp. 1896-1912.

[G-1] Goldstein, C.: "El oficio de los números en los siglos XVII y XIX", *Historia de las ciencias.* M. Serres ed., Cátedra, Madrid 1991, pp. 312-336.

[G-2] —"Autour du théorème de Fermat", en *Mnemosyne*, Université de Paris VII, 7, avril 1994.

[R] Ribenboim, P.: *13 lectures on Fermat´s Last Theorem.* Springer Verlag, Nueva York 1979.

[S] Singh, S.: *Fermat´s Last Theorem* (video). BBC-1997, www.bbc.co.uk./horizon/fermat.shtml

[Wi] Wiles, A.: "Modular ellipic curves and Fermat´s Last Theorem", *Ann. of Math.* V. 141 (1995), pp. 443-551.